Amendment to the Claims:

This listing of claims replaces all prior versions, and
listings, of claims in the application:

1. (Currently Amended) A method to enable a device at a
public network to establish a connection into a private network,
the method comprising:

establishing a persistent connection from an agent
component to a server;

receiving a request from the device across the public
network at the server to establish a connection between the
device and the private network;

determining, at the server, if the device is authorized to
connect with the private network;

if authorized, forwarding the request from the server to
the agent component; and

the agent component creating a connection between the
private network and the device via the server, wherein ~~the agent
component is configured for a dynamically assigned address, and
wherein~~ the server is configured for a persistent address.

2. (previously presented) The method of claim 1 further
comprising the agent component establishing a temporary
connection between the device and a device included in the
private network.

3. (original) The method of claim 1 further comprising, if
not authorized, denying the device access to the private
network.

4. (cancelled)

5. (previously presented) The method of claim 1 in which the persistent connection comprises the server and the agent component having a connection lasting as long as a mechanism at the server and agent component supporting the connection remains active.

6. (previously presented) The method of claim 1 in which the server and the device have a connection lasting as long as a mechanism at the server and a mechanism at the device supporting the connection remain active.

7. (original) The method of claim 1 in which the determining includes authenticating a password.

8. (original) The method of claim 1 in which the public network includes the Internet.

9. (previously presented) The method of claim 1 in which the agent component and the server include proxy servers.

10. (Currently Amended) An article comprising a machine-readable medium which stores machine-executable instructions, the instructions causing a machine to:
establish a persistent connection from a second network component designated with a persistent address to a first network component;
receive a request from a device across a public network at the second network component to establish a connection between the device and a private network;
determine, by the second network component, if the device is authorized to connect with the private network;

if authorized, forward the request from the second network component to the first network component; and

create, with the first network component, a connection between the private network and the device via the second network component, ~~wherein the first network component is configured for a dynamically assigned address~~.

11. (previously presented) The article of claim 10 further comprising the first network component establishing a temporary connection between the device and a device included in the private network, wherein the dynamically-assigned address comprises a dynamic IP address.

12. (original) The article of claim 10 further comprising, if not authorized, denying the device access to the private network.

13. (cancelled)

14. (original) The article of claim 10 in which the first network component and the second network component have a connection lasting as long as a mechanism at each of the components supporting the connection remains active.

15. (previously presented) The article of claim 10 in which the second network component and the device have a connection lasting as long as a mechanism at the second network component and a mechanism at the device supporting the connection remain active.

16. (original) The article of claim 10 in which the determining includes authenticating a password.

17. (original) The article of claim 10 in which the public network includes the Internet.

18. (original) The article of claim 10 in which the first network component and the second network component include proxy servers.

19. (Currently Amended) A system comprising:

a server component configured to connect to a public network and determine if a device is authorized to connect with a private network; and

an agent component configured to establish a persistent connection to the server component and to [[a]]the private network, and further configured to provide [[a]]the device with access to the private network via the server component and the public network, wherein the agent component is configured to connect to the server component prior to connecting to the private network, wherein the agent component is further configured for a dynamically assigned address, wherein the public network has a connection with the device; and wherein the server is assigned with a persistent address.

20. (original) The system of claim 19 in which the agent component is also configured to provide any number of devices configured to connect to the public network with access to the private network via the server component and the public network.

21. (original) The system of claim 19 in which the agent component is also configured to provide the device with access to a device included in the private network.

22. (original) The system of claim 19 in which the server component and the agent component are both extensible to support any protocols used by the public network and by the private network.

23. (original) The system of claim 19 in which the public network includes the Internet.

24. (original) The system of claim 19 in which the server component is also configured to authenticate the device.

25. (original) The system of claim 19 in which the agent component is also configured to maintain a connection with the server component as long as a mechanism at each of the components supporting the connection remains active.

26. (original) The system of claim 19 in which the server component is also configured to maintain a connection with the device as long as a mechanism at the server component and a mechanism at the device supporting the connection remain active.

27. (cancelled)

28. (original) The system of claim 19 in which the agent component is implemented inside the private network.

29. (cancelled)

30. (previously presented) The method of Claim 1, further comprising establishing a connection between the device at the public network and the server after the establishing of the persistent connection from the agent component to the server.

31. (previously presented) The method of Claim 1, further comprising establishing a connection between the private network and the agent before the establishing of the persistent connection from the agent component to the server.

32. (previously presented) The method of Claim 1, wherein the request from the device at the public network travels from the server to the agent prior to reaching the private network.

33. (previously presented) The article of Claim 10, further comprising instructions to establish a connection between the device at the public network and the first network component after the establishing of the persistent connection from the second network component to the first network component.

34. (previously presented) The article of Claim 10, further comprising instructions to establish a connection between the private network and the second network component before the establishing of the persistent connection from the second network component to the first network component.

35. (previously presented) The article of Claim 10, wherein the request from the device at the public network travels from the first network component to the second network component prior to reaching the private network.

36. (previously presented) The system of Claim 19, wherein the connection between the agent and server component comprises a persistent connection.

37. (previously presented) The system of Claim 19, wherein the agent component is implemented within a residential gateway.

38. (previously presented) The system of Claim 37, wherein the server component is implemented within a residential gateway.

39. (previously presented) The system of Claim 38, wherein the private network comprises a secured network.